Practical Guidance

E-discovery: Slack Data Checklist (Federal)

A Practical Guidance® Checklist by
Travis Bustamante, Elaine Yap, and West Lee, Nelson Mullins Riley & Scarborough LLP

Travis Bustamante
Nelson Mullins Riley & Scarborough LLP

Elaine Yap
Nelson Mullins Riley & Scarborough LLP

West Lee
Nelson Mullins Riley & Scarborough LLP

This checklist outlines considerations and processes for responding to a discovery demand seeking the production of Slack messages and files (Slack Data) in a federal court litigation. Specifically, this note covers the scope of production; potential objections to producing Slack Data; and the unique aspects associated with retaining, collecting, exporting, reviewing, and producing Slack Data.

For a related practice note, see E-discovery: Slack Data (Federal).

For more information on e-discovery, see E-discovery: Planning for and Conducting E-discovery (Federal), E-discovery Best Practices (Federal), E-discovery Resource Kit (Federal), Electronically Stored Information: Preserving ESI (Federal), Electronically Stored Information: Collecting ESI (Federal), Electronically Stored Information: Producing ESI (Federal), Electronic Document Review Fundamentals (Federal), Metadata in E-discovery (Federal), and Proportionality in E-discovery (Federal).

What Is Slack?

Slack is a service used to facilitate communication and collaboration in a digital workplace. It is:

- An increasingly common communication tool, particularly during the COVID-19 pandemic –and–
- Revolutionizing how businesses work by supplementing—and in some cases even largely replacing—more traditional communication tools such as email

Slack communications occur in workspaces where free-form discussions take place in real time and can include, among other things:

- Conversational back-and-forth messaging
- Document and other file sharing –and–
- Rapid-fire emoji/symbol response capability

Individuals can transmit Slack Data:

- To large or small groups with varying levels of access –and–
- In direct and multi-person private messages

With Slack's proliferation into the corporate world, you can expect to see discovery requests seeking Slack Data when your client uses Slack to support its business.

Step One: Determining the Scope of Production

Under the Federal Rules of Civil Procedure, a party may serve a request for production of any documents, if the documents are:

- Relevant to the litigation –and–
- In the responding party's possession, custody, or control

Fed. R. Civ. P. 34(a)(1).

Recently, courts have interpreted Rule 34 to find that Slack Data is subject to discovery when the propounding party can demonstrate that the data is:

- Relevant to any party's claim or defense, not privileged, proportional to the needs of the case –and–
- Within the responding party's possession, custody, or control

See, e.g., Laub v. Horbaczewski, 2020 U.S. Dist. LEXIS 247102, at *11–13 (C.D. Cal. Nov. 17, 2020).

Once the propounding party establishes that Slack Data meets Fed. R. Civ. P. 34(a)(1), the responding party must either:

- Produce the requested documents
- Allow for those documents to be inspected –or–
- Object to the request

Fed. R. Civ. P. 34(b)(2). If the responding party objects to the request, the requesting party may bring a motion to compel the responding party to produce the information sought. Fed. R. Civ. P. 37(a)(3)(B). See Laub, 2020 U.S. Dist. LEXIS 247102, at *13–16 (concluding that it could not compel the producing party to consent to the plaintiff's third-party subpoena to Slack).

Courts generally allow parties to obtain non-privileged discovery that is relevant to the party's claim or defense and proportional to the needs of the case when considering the following:

- Importance of the issue
- The amount at issue
- The parties' relative access to relevant information and resources
- The importance of the discovery to resolving the ultimate issue –and–
- The weight of the burden or expense of the discovery in comparison to the benefit

Fed. R. Civ. P. 26(b)(1).

Courts will generally limit discovery if:

- It is unreasonably cumulative or duplicative
- It is burdensome
- There are more convenient ways to obtain the information
- The discovery is outside of the permitted scope –or–
- The party seeking discovery has already had ample time to obtain that information

Fed. R. Civ. P. 26(b)(2)(C). See, e.g., Laub, 2020 U.S. Dist. LEXIS 247102, at *11–13.

For additional practical guidance on proportionality, see Proportionality in E-discovery (Federal).

Techniques to Limit Disputes

In advance of the Fed. R. Civ. P. 26(f) conference, which the federal rules require at the beginning of the case, you should assess:

- Whether Slack is at issue for discovery
- The types of Slack messages that may be at issue –and–
- The tier of Slack that the organization uses

Depending on the level of impact Slack Data has on your litigation, be prepared to either:

- Affirmatively raise how Slack Data will be treated –or–
- Respond to potential requests to include Slack Data during the 26(f) conference or subsequent meet and confers concerning the scope of discovery

If Slack Data will be at issue, you should additionally discuss:

- Whether the producing party will be using a third-party vendor or e-discovery law firm –and, if so–
- What their capabilities are concerning collection, processing, and production of Slack Data

For more information on Rule 26(f) conferences, see Rule 26(f) Conference and Discovery Plan Requirements (Federal) and Rule 26(f) Report and Discovery Plan (Federal).

Important Questions and Considerations

There are several questions you should ask your client that likely will impact collection and production of Slack Data and the proportionality analysis. These questions include defining the following:

- **Documents**. What constitutes a document? Is it a single message? An hour or day's worth of messages? Or is it every message contained within a given channel? How an organization answers this question will impact the volume of Slack Data for collection, as well as the time and amount of work needed to search, process, and review the Slack Data for production.
- **Custodians**. You must identify the custodians for given documents. The Electronic Discovery Reference Model (EDRM) defines "data custodian" as a person "having administrative control of a document or electronic file," and identifies the owner of an email account as the prototypical example. This poses the question of whether an individual user within a given channel is the custodian of their own messages or is the administrator of that channel (if not the user) its custodian? The same question could apply to multiparty messages wherein an individual user, despite being a party to a multiparty message, does not participate. Additionally, is the Slack system itself a "custodian" or can you consider it a noncustodial data source? You should consult with your client to align on an approach for defining data custodians and confirm it is consistent with how your client has previously defined custodians for Slack Data.
- **Contextual relevance**. In an email review, for example, litigants often produce full document families (emails and any attachments) if one file within the family is relevant, even if other members of the family are not. This is done to provide context for the individually responsive document. While Slack communications do not correlate exactly to email, you similarly should provide context for relevant, produced data. Organizations must decide what additional messages or files should be produced alongside relevant Slack messages/files. Options include producing the relevant message or file along with:
  - Any direct thread replies
  - A specified number (e.g., 5 or 10) of messages found directly before and/or after it –or–
  - All other messages or files shared within a certain time period

Step Two: Retention, Collection, Export, Review, and Production

Once Slack Data is in play in your case, you must proceed to the mechanics of retaining, collecting, exporting, reviewing, and producing Slack Data.

In addition to traditional messaging within channels:

- Slack communications occur in the form of file sharing, thread and emoji responses, and other ways –and–
- Users can subsequently edit or delete messages

Note the following:

- Slack records, logs, and tracks user actions such as communications, shared files and images, and any edits and deletions.
- For all but free accounts (which only retain the most recent 10,000 messages), Slack has customizable retention policies that companies can set to fit an organization's preferences or needs.
- The default retention setting retains all messages and files, regardless of whether they are found in public/private channels or in direct/multiparty messages, for the full life span of the workspace. However, you can modify the settings in the following ways:
  - Messages:
    - Keep everything (i.e., messages, revisions, deletions, etc.) forever.
    - Keep all messages, but do not track revisions/deletions.
    - Delete messages and their revisions/deletions after a specified time.
    - Let workspace users set their own retention policies.
  - Files:
    - Keep all files.
    - Keep all files for a certain number of days.

For information on documentation retention and litigation holds, see Litigation Hold Resource Kit (Federal).

Collection and Export

Companies currently have two methods to collect Slack Data:

1. A workspace administrator requests an export of data from Slack. –or–
2. The company uses Slack's discovery application programming interface (API) or other integrated collection application, such as Relativity Collect.

Data Export

The ability of a workspace administrator to collect and export data from Slack is tied, at a basic level, to the type of Slack account the organization has.

You can collect Slack Data through a standard export if your client has the following Slack accounts:

- **Free account.** These are used primarily by smaller organizations. Administrators only have access to perform a standard export of the 10,000 most recent messages, though the Slack tool itself still retains all workspace data. For access to export all workspace data, free plan administrators must provide valid legal process, consent of members, or evidence of a legal requirement/right, and must request the Slack Data from Slack.
- **Standard account.** These are used by smaller and medium sized organizations. Standard exports provide all public channel content from a workspace, including messages and links to files that have been publicly shared, as well as edit and deletion logs for public messages only. However, standard exports do not provide messages and files shared in private channels, messages and files shared in direct or multiparty messages, or metadata related to edits/deletions of private messages. For access to export all workspace data, standard plan administrators must provide valid legal process, consent of members, or evidence of a legal requirement/right, and must request the full Slack Data from Slack.

Additionally, for standard exports, you can only limit the Slack Data collection by date range.

You can collect Slack Data through a corporate export if your client has the following Slack accounts:

- **Plus account.** These are used by smaller and medium sized organizations. In addition to having access to export all data that standard plans do, plus plans can perform corporate exports, which allow exports from private channels and direct/multiparty messages (including shared messages, files, and edit/deletion logs). However, as with standard plan users, plus plans can only limit the Slack Data collection by date range.
- **Enterprise grid account.** These are used by larger organizations. With enterprise grid accounts, companies can do everything that plus plans can do, as well as work with integrated collection applications, and further target and limit collections by select individual users or channels.

Strategic Considerations

You should identify and discuss the following key items before collecting the Slack Data:

- **Metadata.** No matter what tool you use to collect Slack Data, you should verify that you will receive complete and accurate metadata for Slack Data at the time of collection. For more information on metadata in e-discovery, see Metadata in E-discovery (Federal). Note the following:
  - Failing to receive accurate metadata can create significant downstream issues. For example, the basic unit of metadata used for attributing Slack messages to a particular user is the User ID, a series of random numbers and letters that do not reflect a user's name, which is the value most commonly used to assign custodian values.
  - Accurate metadata is also critical to determine message transmission dates; the manner of transmission (public or private channel, direct, or multiparty message); and message or attachment status, all of which you will need to scope your collection, review, and production.
- **Relativity Short Message Format (RSMF).** Occasionally, more sophisticated companies convert Slack Data exports into Relativity Short Message Format (RSMF) before providing it to their technology partners. Before recommending this option to your client, you should verify that the company has the tools to appropriately export Slack Data. Note the following:
  - Once Slack Data converts to Relativity Short Message Format (RSMF), you likely cannot further cull or process the data.
  - If your client uses a conversion tool and fails to capture accurate custodial metadata prior to

conversion, you likely cannot recreate the custodial information without the original raw Slack Data.

- In these situations, you should request a copy of the raw Slack Data export from the client.

Responding parties should continually evaluate the cost and burden associated with Slack Data and analyze how those costs and burdens are proportional to the needs of the case.

For more information on collecting ESI, see Electronically Stored Information: Collecting ESI (Federal).

Review

Once you have collected, exported, and converted Slack Data into a workable format, reviewing Slack Data is similar to reviewing documents from traditional data sources. For example, in Relativity, once Slack Data is converted into Relativity Short Message Format (RSMF), you can review it in the workspace similar to email, Skype, or text message data. You can utilize viewer and extracted text modes, which allow for keyword and index searching. However, you should consider the following before commencing your review:

- First, standard culling methods will not have the same impact with Slack Data as they would with email. For example, you cannot thread Slack messages, and successful de-duplication depends on a number of factors including the method of collection and retention policies, both of which can vary more widely with Slack than traditional data sources.
- Second, much like text messages, Slack users typically communicate in a less formal manner than email. Accordingly, you may have difficulty identifying who is speaking within a channel, direct message, or multiparty messages. The following examples highlight these issues:
  - In a matter where one of the relevant topics is the corporate review of financial statements, you might normally run a search for all documents hitting on the following search term: ((review* or analy*) w/5 (financ* or statement*)). You could also consider applying highlighting to various terms or phrases to aid reviewers. However, a Slack communication regarding review of financial statements could conceivably present as—User 1: What's the status of those financials? User 2: [replies with a GIF of a man holding a magnifying glass up to a stack of papers]. While this exchange could mean that the financial statements are currently undergoing review, no combination of search terms or highlighting would effectively isolate this exchange.
  - In many reviews, attorney names and other terms and phrases likely implicating privilege will be run as a search term report and added to term highlighting. However, because Slack communications are (1) between users capable of customizing their handles such that they may mask their identity, and (2) significantly less formal than email, such that even when attorneys are referenced, they frequently are not called by their full names, this standard approach to identifying potentially privileged material is less effective when reviewing Slack Data than more traditional e-discovery reviews. Accordingly, if Slack Data is part of your case, you will likely have to conduct a full review of the potentially relevant messages to confirm relevance and identify privileged content.
- Third, the conversational nature of Slack messages means the context around the message has increased importance. Thus, note the following:
  - When users communicate in Slack, they rarely monologue or speak in complete paragraphs such that a fully formed idea is exchanged in one volley. Instead, users communicate in half sentences, expressions (memes), and other rapid-fire ways. Often, users spread a full discussion throughout a channel or multiparty conversation. Similarly, a single Slack message may not seem particularly important at first glance, but if you review the 10 or 20 messages surrounding it, the single message could suddenly take on a relevance not apparent without the contextual messages.
  - You should build a review workflow that incorporates context into your Slack messages review. You can do this during collection by deciding that a document is not limited to a single message, but rather a set number of messages or a set time period. You then process the Slack Data accordingly so that a reviewer will have the number of messages or the messages from a set period of time that you decide best assists the review team.
  - If you decide that documents should be limited to single messages, you can still provide context by building out certain parameters for review:
    - For example, while families will not be presented the same as they would be with email (with the

limited exception of messages actually attaching a file), technical partners can create similar relational groups that will present a given message hitting on search terms in a block of 10, 15, or whatever number of surrounding messages you deem appropriate.

    - While a larger number of messages presented together increases the chance of having the necessary context to make a fully informed decision, you should balance this with the diminishing returns experienced when providing too much information.

- Finally, you will need to instruct your review team how to treat emojis and to elevate questions about the impact of emojis. Slack users frequently use emojis to acknowledge receipt of information and approve content and the reaction can be critical to discovery. You should incorporate into your review guidelines and training a section about emojis to make sure that reviewers who are new to Slack understand the importance of emojis and that the team consistently codes documents that have emojis.

Reviewing Slack Data can often be more burdensome than reviewing traditional electronic communications and you should evaluate whether reviewing Slack Data is proportional to the needs of the case.

Production

The process to run a Slack production largely mirrors production workflows for more traditional data sources, for example:

- You can image messages and group them together in various ways to form families
- You can produce shared files natively, where necessary (such as with excel files shared in Slack channels)
- The metadata for each Slack message, when collected appropriately, can be included in a load file corresponding to a TIFF image production of Slack messages

For more information in producing ESI, see Electronically Stored Information: Producing ESI (Federal).

Related Content

Practice Notes

- Electronically Stored Information: Authenticating ESI (Federal)
- Electronically Stored Information: Collecting ESI (Federal)
- Electronically Stored Information: Preserving ESI (Federal)
- Proportionality in E-discovery (Federal)
- E-discovery Best Practices (Federal)
- Electronic Document Review Fundamentals (Federal)
- Metadata in E-discovery (Federal)
- Social Media in E-discovery (Federal)
- Technology-Assisted Review: Overview (Federal)
- Discovery Planning and Strategy (Federal)
- E-discovery: Planning for and Conducting E-discovery (Federal)
- Case Management Conferences (Federal)
- Motion for Protective Order: Making the Motion (Federal)
- Motion Practice: Making and Opposing a Motion (Federal)

Annotated Forms

- E-discovery Production Format Protocol (Federal)
- Document Retention Policy (Federal)
- Litigation Hold Notice (Federal)
- Rule 26(f) Report and Discovery Plan (Federal)
- Complaint (Federal)
- Answer (Federal)

Checklists

- E-discovery Vendor Checklist (Federal)
- E-discovery Project Management Checklist (Federal)
- Email Threading in E-discovery Checklist (Federal)
- Electronically Stored Information: Processing ESI Checklist (Federal)
- E-discovery: Planning for and Conducting E-discovery Checklist (Federal)
- Document Retention Policy Checklist (Federal)
- Litigation Hold Notice Checklist (Federal)
- Rule 26(f) Conference and Discovery Plan Requirements Checklist (Federal)
- Managing Civil Litigation Checklist (Federal)
- Motion Practice: Making and Opposing a Motion Checklist (Federal)
- Discovery Tools Comparison Chart (Federal)
- Discovery Strategy Checklist (Federal)
- Scope of Discovery Checklist (Federal)

Travis Bustamante, Partner, Nelson Mullins Riley & Scarborough LLP

Travis A. Bustamante's litigation practice focuses on electronic discovery, data breach response efforts, information governance, and litigation readiness. He works with clients in state and federal courts on issues of discovery strategy and provides counsel regarding legal holds and data preservation, fact investigations, deposition preparation, meet and confers, discovery motions practice, and document productions.

Travis's experience includes counseling Fortune 500 healthcare, financial services, and pharmaceutical clients in large-scale litigation and in response to government inquiries during all phases of the electronic discovery reference model. Pre-litigation, he counsels clients on strategies to address the ever-growing volume of data and defends those strategies in the event they face challenges during future litigation.

Travis also has experience counseling clients in response to data breaches and developing tailored discovery strategies to respond to litigation and regulatory requirements. He frequently advises clients on developing defensible strategies to preserve the attorney-client privilege and work product.

Elaine Yap, Associate, Nelson Mullins Riley & Scarborough LLP

Elaine Yap focuses her practice in the areas of product liability, including pharmaceutical and medical device litigation, and e-discovery.

West Lee, Encompass Discovery Counsel and Project Manager, Nelson Mullins Riley & Scarborough LLP

West Lee is a member of the Encompass Project Management team at Nelson Mullins. He has experience coordinating with clients and case counsel, as well as training and leading review teams of all sizes in a wide variety of large-scale e-discovery matters relating to antitrust, intellectual property, and products liability law, among others. West also manages privilege reviews involving multijurisdictional privilege standards.

This document from Practical Guidance®, a comprehensive resource providing insight from leading practitioners, is reproduced with the permission of LexisNexis®. Practical Guidance includes coverage of the topics critical to practicing attorneys. For more information or to sign up for a free trial, visit lexisnexis.com/practical-guidance. Reproduction of this material, in any form, is specifically prohibited without written consent from LexisNexis.

LexisNexis.com/Practical-Guidance

LexisNexis®

LexisNexis, Practical Guidance and the Knowledge Burst logo are registered trademarks of RELX Inc.
Other products or services may be trademarks or registered trademarks of their respective companies. © 2021 LexisNexis